OIT-DIS/ Risk and Compliance (R&C) Team Group

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

NIST-Risk Management Framework (RMF) Authority to Operate (ATO) IHS-Systems

Presented by	Sam Tharakan Mathew
Title	R&C Federal Team Lead/ Manager
Phone	(301) 526-8489
Email	Sam.Mathew@ihs.gov
Team Email	IHSDISRiskAndCompliance@ihs.gov
Target Date	***14 August 2024***
Target Start Time	***08 :00 AM EST***

Indian Health Service (IHS) / Office of Information Technology (OIT)/ Division of Information Security (DIS)

DYK? – Phoenix, Arizona!

What is Phoenix, Arizona famous for?

- Possibly as early as 300 BC, the Hohokam were the earliest permanent Native American inhabitants of the Phoenix area and remained until about AD 1400. After them came the Akimel O'odham (Pima), Maricopa, Yavapai, and Yaqui groups.
- The Grand Canyon inspired the architecture of the Phoenix Convention Center - The red rock walls and turquoise waters of the Grand Canyon inspired the architecture of the Convention Center when it was expanded in 2008. The $600 million project tripled the size of the center to more than 900,000 square feet of extraordinary meeting and exhibit space.
- Phoenix, the capital of the U.S. state of Arizona, has 58 completed high-rises taller than 200 feet (61 m). The tallest building in Phoenix is the 40-story Chase Tower, completed in 1972 with 38 habitable floors rising to 483 feet (147 m). It is also the tallest building in Arizona.
- Phoenix Suns, American professional basketball team bas Established in 1968, the Suns play in the National Basketb (NBA) and have won three Western Conference titles (19 2021).
- …etc (Larry Fitzgerald Jr. –17 seasons/ AZ Cardinals NFL)

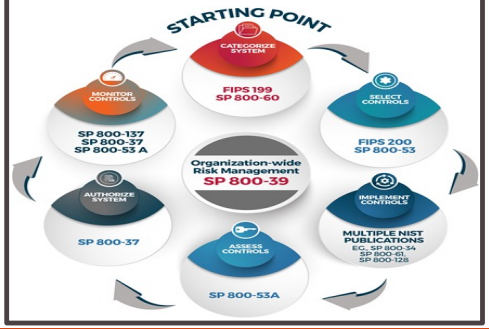
OIT-DIS Risk & Compliance Team

The Risk and Compliance (R&C) Team D2D Roles & Responsibilities:

- ✓ Aligns to the IHS-DIS objectives while managing the cyber risks, in order to achieve the regulatory needs (FISMA/HIPAA/GAO/A-123/OIG/BOD/HHS = 7+).
- ✓ Improves the security of IHS data by identifying gaps, categorizing and documenting security risks that have the potential to impact IHS's ability to satisfy its mission, vision, goals and priorities.
- ✓ Establishes governance, formality, ownership, and accountability by developing, conducting and updating security assessments for IHS-HQ and other related national systems.

R&C Links

- R&C SharePoint Site
- R&C Security Publications
- NIST 800-37 RMF
- NIST 800-53 InfoSec
- Archer GRC
- IHS Front Lines



Who's your PoC at the Risk & Compliance Team?

Sam Tharakan Mathew | MS, PMP, CISM, CISA, CASP+, CEH

Sam comes with a broad and diverse background in IT-OT engineering. He has attained his masters degree with multiple industry certifications in both IT-OT and project management. Over 15 years, Sam has significantly contributed as a key senior management consultant to the IT-OT cybersecurity programs at various private sectors and Federal Nuclear Energy facilities. Sam was also a member of the LexisNexis management team, where he established the LNRT organization's first global GRC & Audit Department, which was responsible for overseeing and assisting the Federal USPTO's ATO mission, amongst other commercially globalized healthcare, intellectual property and financial compliance frameworks.

IHS/ NIST Acronyms & Abbreviations

Glossary | https://csrc.nist.gov/glossary

Acronym	Definition
AO	Authorizing Official
ATO	Authorization to Operate
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
CMP	Change Management Plan
CSP	Cloud Service Provider
DRCP	Disaster Recovery and Contingency Planning
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISCP	Information System Contingency Plan
ISSO	Information System Security Officer

Acronym	Definition
NIST	National Institute of Standards and Technology
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SAP	Security Assessment Plan
SAR	Security Assessment Report
SCA	Security Control Assessor
SO	System Owner
SP	Special Publication
SSP	System Security Plan
ST&E	Security Testing and Evaluation

What is the World's Most Valuable Commodity?

- **D.A.T.A.** is now becoming the most valuable commodity on earth, surpassing fossil fuels like oil… etc
- The **BIG TECH giants** that deal in data, such as Google, Amazon, Facebook, Apple, Microsoft and Tesla, are **becoming increasingly powerful**.
- Ai?
  - ***DYK?*** *An individual's Facebook data may be worth over $100, and one individual sold his data for $2,733 on Kickstarter.*

Regulating the internet giants

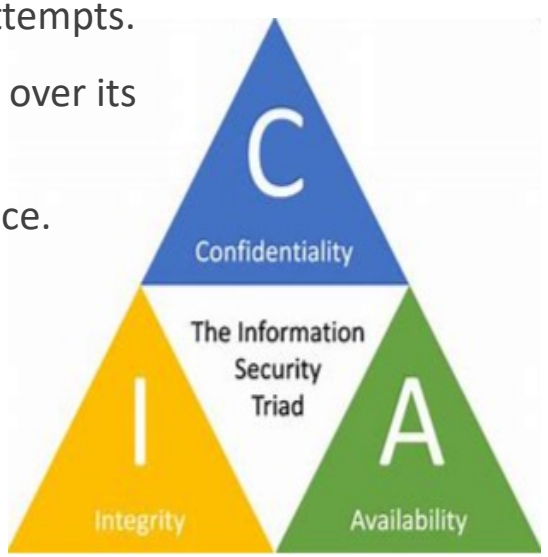
The world's most valuable resource is no longer oil, but data

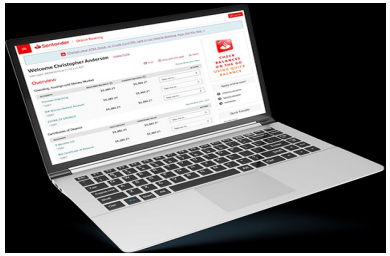
The data economy demands a new approach to antitrust rules

The C.I.A = ?

Confidentiality/ Integrity/ Availability (CIA) is a **benchmark model** that governs how the IHS protects it's information systems and data.

- **Confidentiality** prevents privacy information from unauthorized access attempts.
- **Integrity** maintains the consistency, accuracy and trustworthiness of data over its entire lifecycle of service delivery
- **Availability** refers to the readiness of data that is required to deliver service.





***NOTE**: Consider an online banking account as an example.*

*It is critical that the user's information is secret (**confidentiality**), accurate (**integrity**) and accessible (**availability**) at all times.*

IHS' Mission/ Vision/ Goals?

-
-
-

Indian Health Service
The Federal Health Program for American Indians and Alaska Natives

Search IHS

A to Z Index | Employee Resources | Feedback

The Indian Health Service is working closely with our tribal partners to coordinate a comprehensive public health response to both COVID-19 and mpox.

About IHS | Locations | *for* Patients | *for* Providers | Community Health | Careers@IHS | Newsroom

About IHS / Agency Overview

About IHS

- Agency Overview
- Annual Budget
- Eligibility
- Key Leaders
- IHS Calendar
- Indian Health Manual
- Organizational Structure
- Our Employees

Agency Overview

The Indian Health Service, an agency within the Department of Health and Human Services, is responsible for providing federal health services to American Indians and Alaska Natives. The provision of health services to members of federally-recognized tribes grew out of the special government-to-government relationship between the federal government and Indian tribes. This relationship, established in 1787, is based on Article I, Section 8 of the Constitution, and has been given form and substance by numerous treaties, laws, Supreme Court decisions, and Executive Orders. The IHS is the principal federal health care provider and health advocate for Indian people, and its goal is to raise their health status to the highest possible level. The IHS provides a comprehensive health service delivery system for American Indians and Alaska Natives.

Related Information

- Fact Sheets

Our Mission: to raise the physical, mental, social, and spiritual health of American Indians and Alaska Natives to the highest level

Our Vision: healthy communities and quality health care systems through strong partnerships and culturally responsive practices

Strategic goals:

- to ensure that comprehensive, culturally appropriate personal and public health services are available and accessible to American Indian and Alaska Native people;
- to promote excellence and quality through innovation of the Indian health system into an optimally performing organization; and
- to strengthen IHS program management and operations

3-TIER RISK MANAGEMENT

NIST SP 800-39, Chapter 2, Section 2.2, Managing Information Security Risk: Organization, Mission, and Information System View

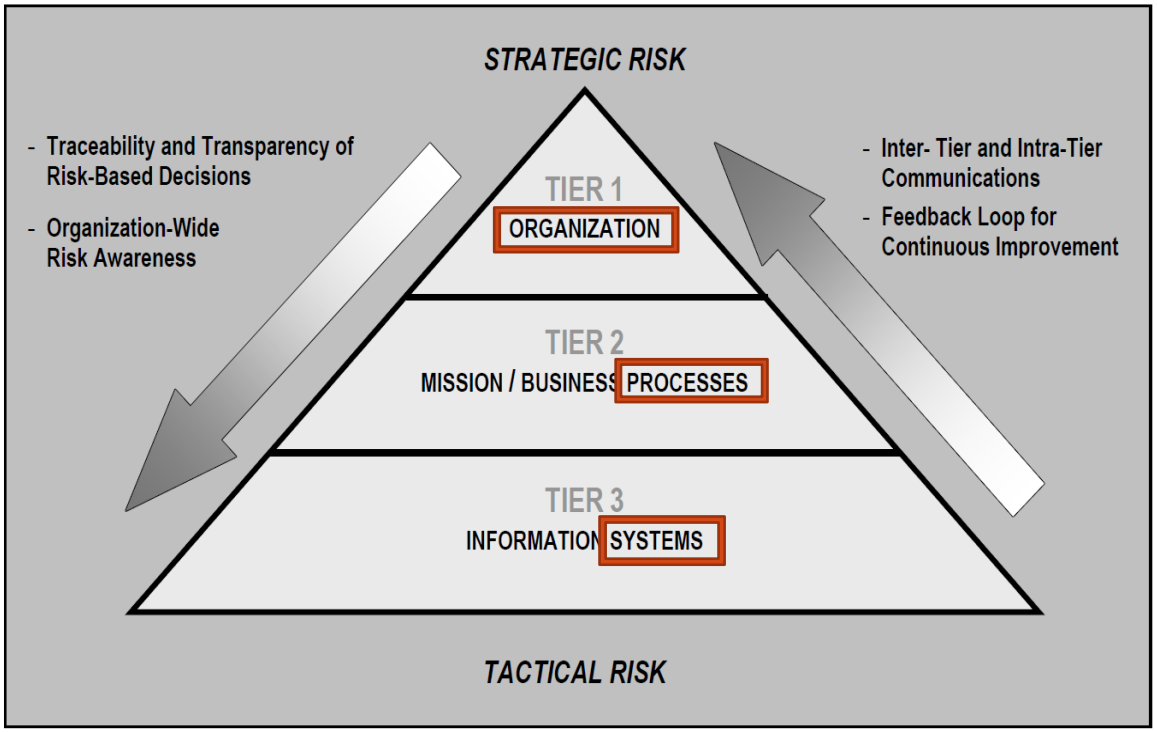
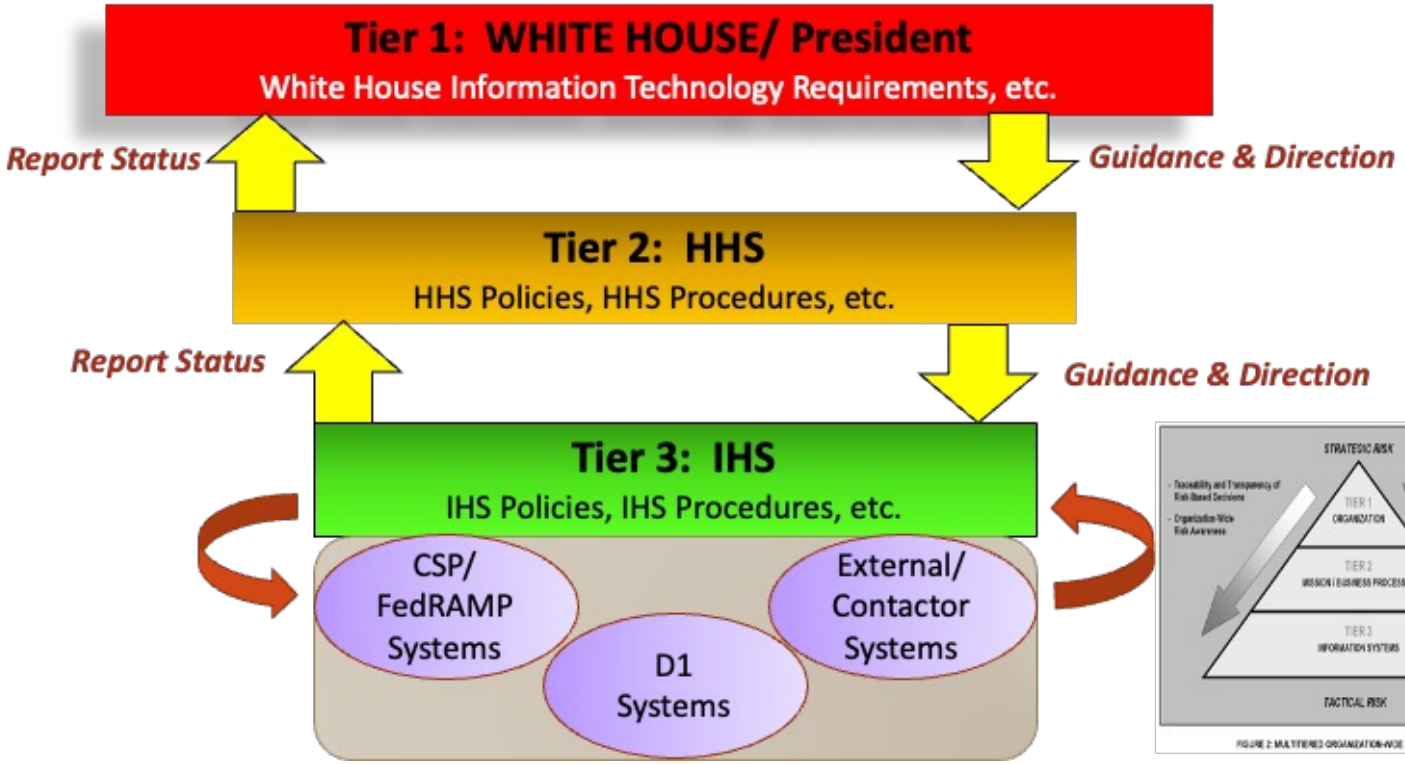


FIGURE 2: MULTITIERED ORGANIZATION-WIDE RISK MANAGEMENT

- **Tier-1** provides a prioritization of missions/business functions which in turn drives investment and funding by strategic and tactical ***decisions***.
- Thus, Tier-1, affects the development of enterprise/ InfoSec ***architecture*** at **Tier-2**
- Allocations and deployment of ***management***, ***operational***, and ***technical*** security controls at **Tier-3**

IHS' 3-TIER SYSTEM



What types of Information Systems gets ATO?

- NIST-SP-800-18 (S2.2 & 2.3) Classify:

1) General Support System (GSS) – usually the main enterprise network (router, switches, servers, workstations). Usually included email and normally installed applications/ software.

2) Major/ ~~Minor~~ Applications (MA) – This could be in-house applications or business divisions that may have their own sub systems or could actually be applications (DevOps, etc). It can also include cloud/CSP systems, via FedRAMP to IHS-D1 with shared controls matrix.

- Usually MAs would inherit certain controls from the GSS and might have other controls that differ from the GSS.
- Both of these 2 types typically will have the HW/SW/Users in common.

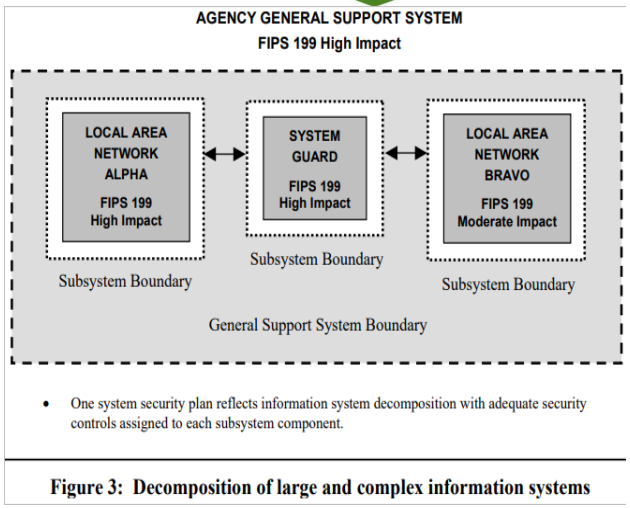


Figure 3: Decomposition of large and complex information systems

3 Types of ATO status at IHS

1) iATO = Initial ATO
   - Must be done prior to the system "going-live" and must occur at least every 3 years thereafter.
   - New system or pre-existing legacy system discovered

2) cATO = Interim/Conditional ATO
   - Generally in effect for 6 months, often during the development or prototype phase.
   - &/or is usually issued to a system where too many outstanding issues were found (especially Critical & High risks).

3) ATO = Full/ Re-Authorization to Operate (ATO)
   - This is the end goal for every system.
   - These ATOs are typically issued for 3 years, at which point they must be recertified annually via ConMon or a significant change to the system's risk level.

Figure 6—RMF Steps for ATO

Security controls are the management, operational and technical safeguards or countermeasures employed within an information system to protect the confidentiality, integrity and availability of the system and its information.[2,23]

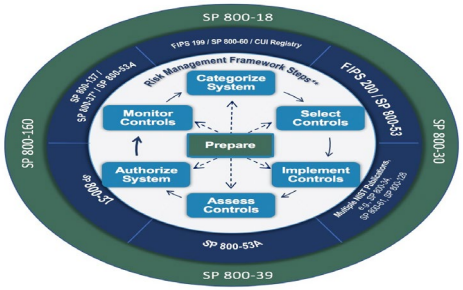
RMF	SP 800-37 Rev. 1	"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"[24]
Step 1: CATEGORIZE Security impact value (low, moderate, high) for the security objectives of confidentiality, integrity or availability		
	FIPS 199	"Standards for Security Categorization of Federal Information and Information Systems"[25]
	SP 800-60	"Guide for Mapping Types of Information and Information Systems to Security Categories"[26,27]
Step 2: SELECT Choosing a set of baseline security controls and specifying minimum assurance requirements (safeguards or countermeasures employed), as appropriate.		
	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems[28]
	SP 800-53 Rev 4	"Security and Privacy Controls for Federal Information Systems and Organizations"[29]
Step 3: IMPLEMENT Controls are: A. Implemented/Compensated/Planned B. System Specific/Inherited/Hybrid		
	SP 800-160	Draft document
Step 4: ASSESS By verification of evidence, test that the controls are in place and operating as intended.		
	SP 800-53A	"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans"[30]
Step 5: AUTHORIZE		
	SP 800-37	"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"[31,32]
Step 6: MONITOR POAMS		
	SP 800-137	"Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"[33]

Source: J. Sorrentino. Reprinted with permission.

ATO Process Steps & Knowing the IT Governance Frameworks

To understand the ATO process, one needs to understand the IT governance frameworks.
The required steps for conducting the ATO security authorization process are:

1) Categorize the information systems in the organization, i.e., determine the criticality of the information system based on potential adverse impact to the IHS business.
2) Select baseline security controls (L/M/H).
3) Implement these security controls, i.e., within the IHS's enterprise architecture.
4) Assess the security controls to determine their effectiveness.
5) Authorize the system.
6) Monitor the system.



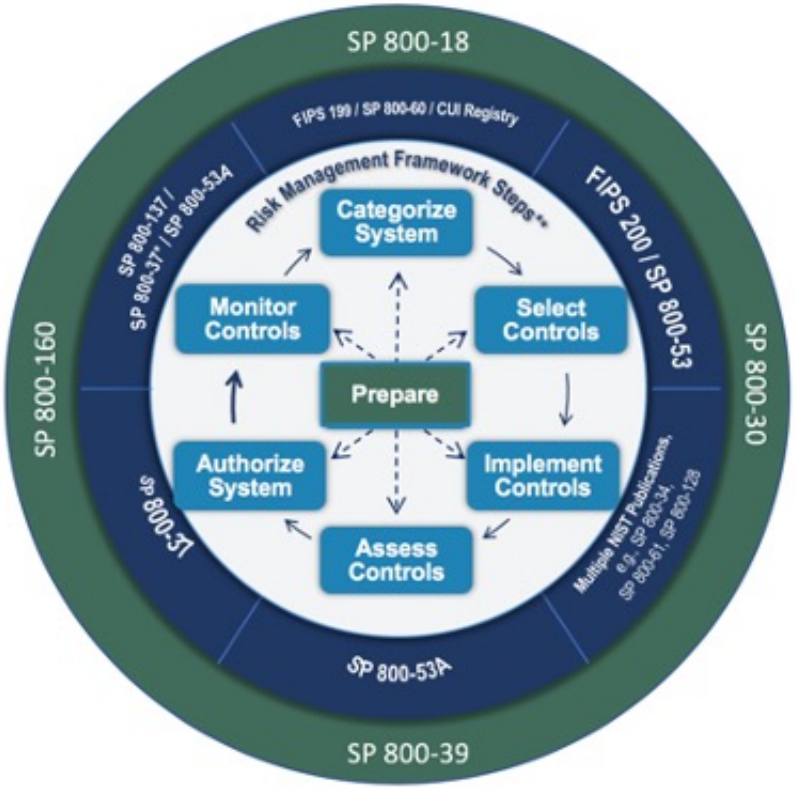
The information security team works to gather the documentation for the system project deliverables from the phases (planning, requirements, design, development, testing, implementation and maintenance) of the Software Development Life Cycle (SDLC) or System Engineering Life Cycle (SELC) frameworks.
This information is needed as documentation in the ATO process and shows evidence of the categorize, select, implement and assess steps while simultaneously fulfilling the stated IT governance frameworks.

NIST-800-37/ Risk Management Framework

The National Institute of Standards and Technology (NIST Risk Management Framework (RMF) 800-37, provides **guidelines** that help ~~businesses and~~ government agencie comply with Federal Information Processing Standards (FIPS) requirements for information systems and data an NIST Special Publication 800-39 requirements.

The NIST RMF consists of the following 6-Prep Steps:

- Step 1: Categorize Information Systems
- Step 2: Select Security Controls
- Step 3: Implement Security Controls
- **STEP 4: ASSESS SECURITY CONTROLS**
- **Step 5: Authorize Information System**
- **Step 6: Monitor Security Controls**



Why Do You Need Your System to be Authorized?

A properly authorized system provides IHS the following benefits:

- Adheres to federal security compliance guidelines: System states – Risk Awareness/ Avoidance/ Acceptance/ Transfer, (Vendor, Cloud/ FedRAMP)
- Helps IHS define and maintain its asset inventory.
- Aligns with the IHS's mission, vision and strategic goals.
- Facilitates the appropriate level of system protection.

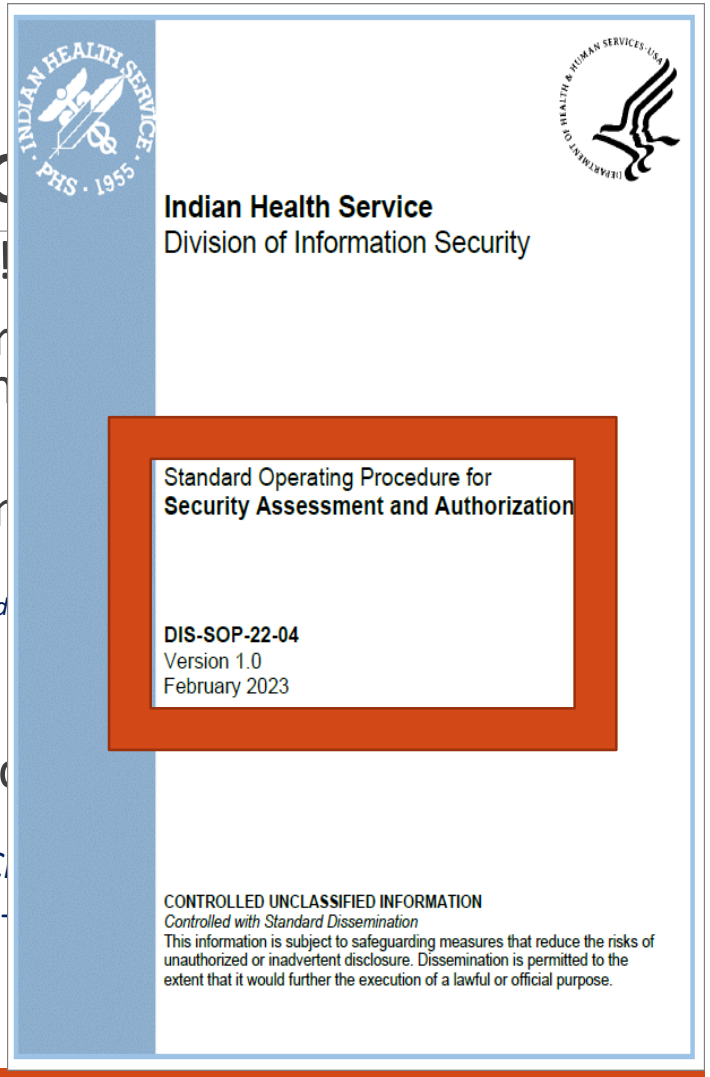
Obtaining System Authorization

To obtain an IHS system authorization, perform the following tasks:

- Work with the Division of Information Security's **ISSOs**!
- Ensure that the System Owner/Division Director has:
  - Officially registered the system in the [*RSA Archer*] Governance, Risk & Compliance (GRC) system
  - Provided an HHS-IHS Universal Unique Identifier.
- **Integrate information security in the system design and development.**
- Complete and assemble required system documentation: start **6-8 months** prior to assessment start date.
- Conduct an initial full-scope assessment 3 months prior to deploying the system in a production environment.
- Continue to work with the Division of Information Security's ISSOs, R&C team to complete a System Assessment Report (SAR) and submit it to the AO/CIO to request an ATO/iATO.

R&C Team' Playboo

- It is the System' - Security Assessment Plan (SAP)!!
- The SCA/ R&C Assessment Team is on hand to carr evaluation that complies with NIST-RMF, by utilizin methods described in NIST publications.
- In order to execute the SA&A process efficiently ar core references are utilized by R&C.
  - NIST-SP-800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and*
  - NIST-SP-800-115, *Technical Guide to Information Security Testing and Assessment*
  - NIST-SP-800-137A, *Assessing InfoSec Continuous Monitoring (ISCM) Programs*
- The primary source of "R&C Team" verification an the following:
  - Big-5-Plans: System' SSP [PL-2] **+** *IRP [IR-8], CMP [CM-9], ISCP [C*
  - System boundary Inventory [CM-8], against the scan results [RA-
  - **HHS-IS2P Baseline (OpDiv) Rev5/ IHS-DIS T&M Handbook**
  - 3-Tier Common Controls, Policies and Procedures



NIST 800-12

An Introduction to Information Security

- In accordance with **Section 5** of the National Institute of Standards and Technology (NIST) Special Publication (SP) **800-12**, Revision 1, structuring policies and procedures should be as follows:

- **Program Policy** – is used to create an organization's information security program. Program policies set the strategic direction for security and assign resources for its implementation within the organization.
  - **These policies will be approved and issued by the CISO** to establish or restructure the Information Security Program.
  - Examples of these policies would be high level like access control, risk management and media sanitizing.
  - All IHS systems would follow these same policies and use them in their respective certification packages.

- **Issue Specific Policy** – There are many areas for which issue-specific policy may be appropriate.
  - New technologies and the discovery of new threats often require the creation of an issue-specific policy.
  - Examples of issue specific policies are email privacy, social media, Bring Your Own Device (BYOD), etc.
  - **These policies will also be approved and issued by the CISO as they affect IHS as a whole.**

- **System Policy** – While program and issue-specific policies are broad, high-level policies written to encompass ALL, system-specific policies provide information and direction on what actions are permitted on a particular system.
  - System policies dictate exactly how a system or component of the system will be securely configured.
  - Note, that one system specific policy could cover multiple systems, for example, a DISA-STIGs could be mandated for all systems, and specific STIGs or benchmark could be issued for specific system components (Windows, Linux, etc.).
  - **System policies should be crafted by the more technical personnel and may not be formally approved by CISO.**

- **DIS-PSA Team Function** – Before any policy goes to the CISO, the PSA Team will vet the policy against industry standard and best security practices and recommend change if any shortcoming is found to streamline the approval process.

NIST 800-53, Rev 5 Controls

- IHS conducts assessments on a 3-year cycle.
- Each year, IHS assesses one third of the controls along with any additional volatile controls.
- **NIST SP 800-53, Revision 5 provides a catalog of security controls grouped in control families. It also defines hundreds of control enhancements.**
  - *High baseline = 170 controls;*
  - *Moderate baseline = 159 controls;*
  - *Low baseline = 115 controls*

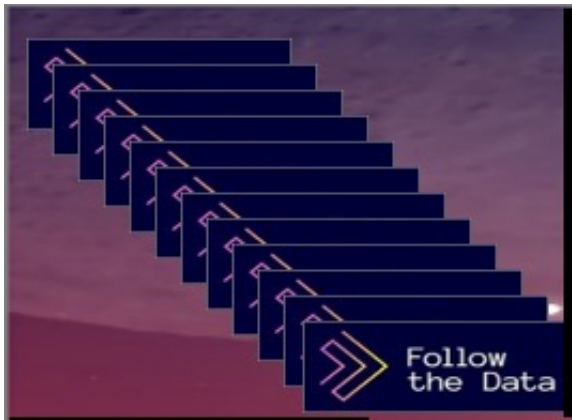
ID	Control Family	ID	Control Family
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	*PT(R5)	Personally Identifiable Information Pro and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	*SR(R5)	Supply Chain Risk Management

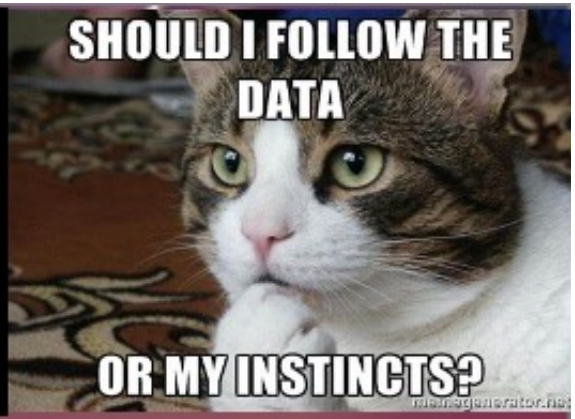
ATO Pre-Assessment Required Documents

The following documents needs to be provided before a System' Security Assessment in conducted, in order for the R&C' Security Control Assessor (SCA) to perform the ATO assessment.

Pre-Assessment Documents	
Document Name/Type	**Stakeholders**
Cloud/FedRAMP (if applicable) – **Rev 5**	System Owner (SO), Information System Security Officer (ISSO), Chief Information Security Officer (CISO)
Privacy Impact Analysis (PIA)	SO, PO
Interconnection Security Agreement (ISA)	SO, ISSO, Interconnected System SO
System Security Plan (SSP) – **Rev 5**	SO, ISSO
Information System Contingency Plan (ISCP)	SO, ISSO, Disaster Recovery & Contingency Planning (DRCP)
Configuration Management Plan (CMP)	SO, ISSO, DRCP
Incident Response Plan (IRP)	SO, ISSO, DRCP

Follow The “What/Who”?





ATO Post-Assessment Required Documents

The following documents are collected after a System Security Assessment. These documents comprise the ATO package.

Post-Assessment Documents	
Document Name/Type	**Stakeholders**
Security Assessment Plan (SAP)	SO, ISSO, SCA
Security Testing and Evaluation (ST&E)	SO, ISSO, SCA
Security Assessment Report (SAR)	SO, ISSO, CISO, SCA
Plan of Action and Milestones (POA&M)	SO, ISSO, CISO, Audit Response & Coordination (ARC)
Authorization to Operate (ATO) Memo	AO, CISO, SO, ISSO, SCA

Assessment Workflow Diagram (RMF Step 4)

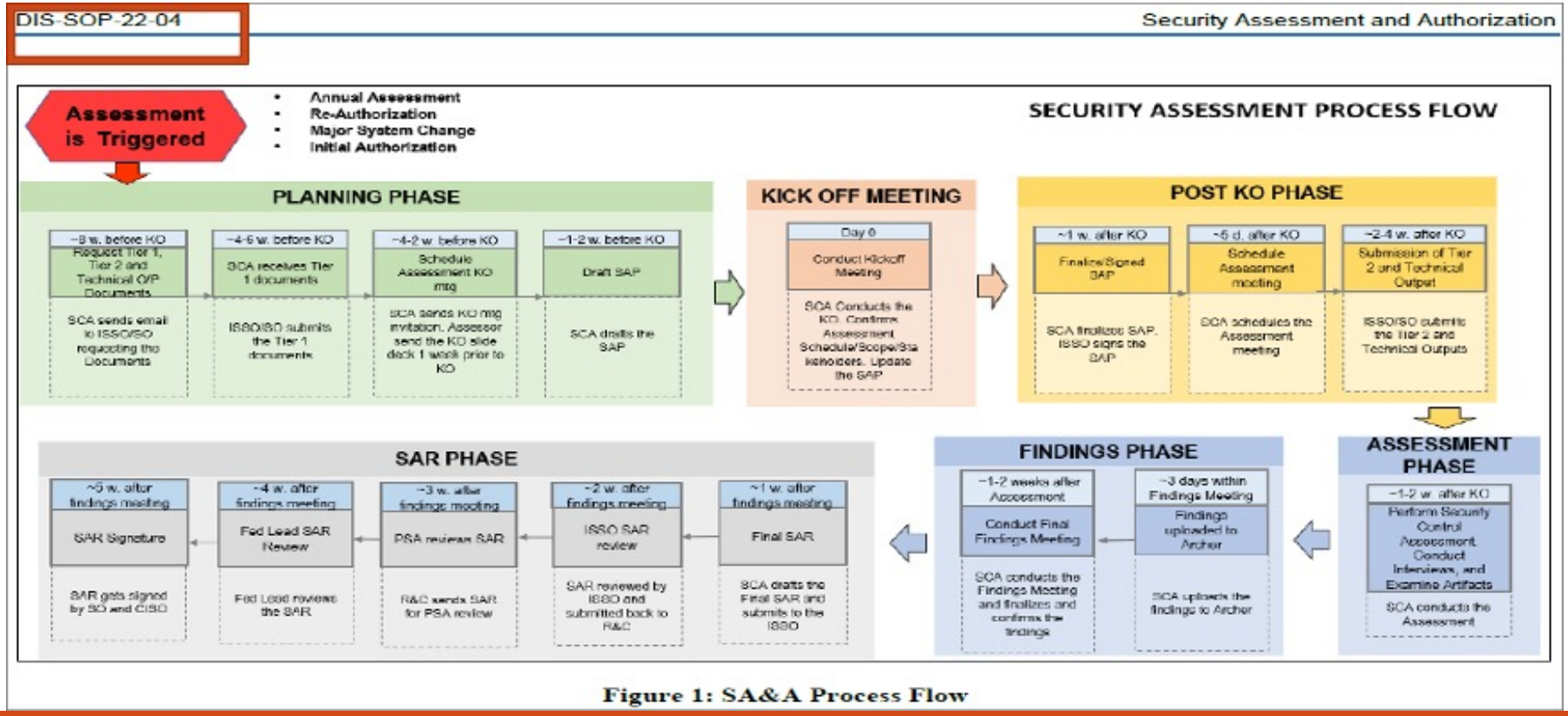


Figure 1: SA&A Process Flow

"Future" Assessment Workflow

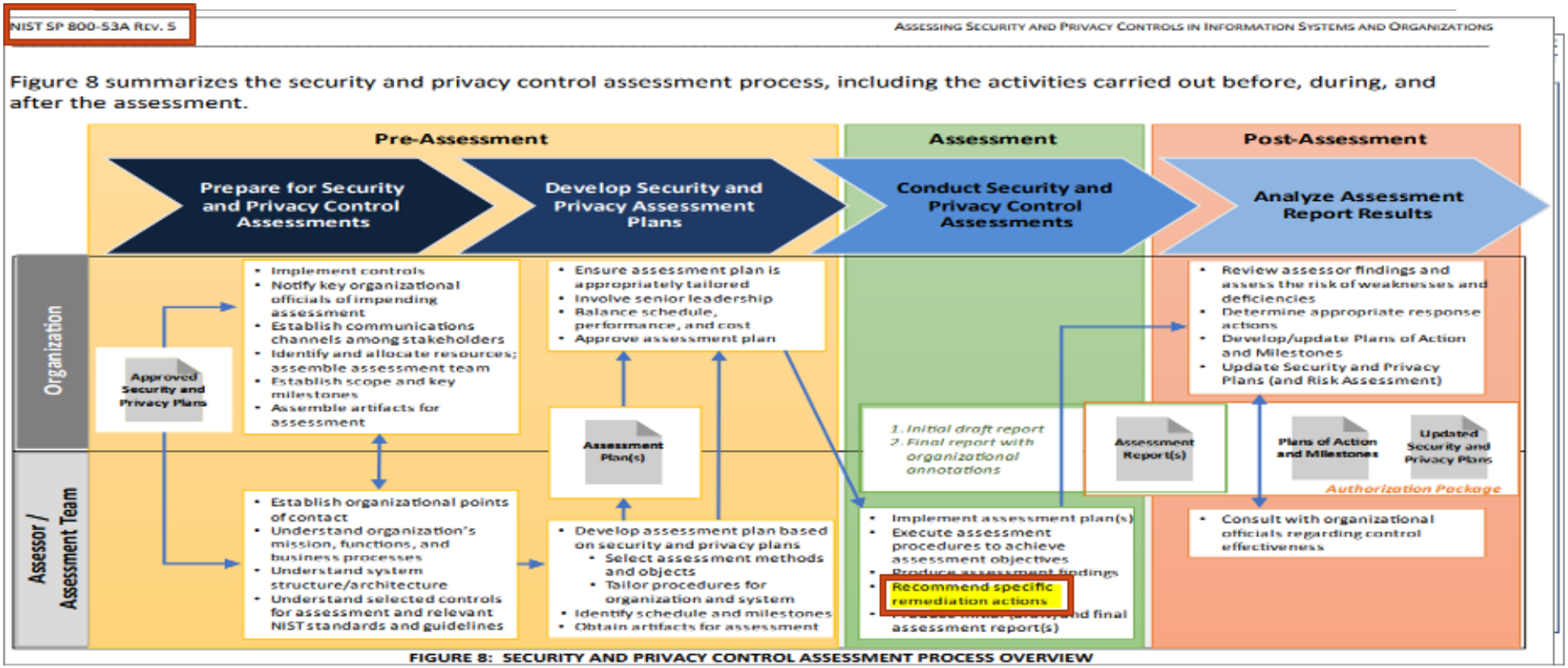


FIGURE 8: SECURITY AND PRIVACY CONTROL ASSESSMENT PROCESS OVERVIEW

NIST SP 800-55

Performance Measurement Guide for Information Security

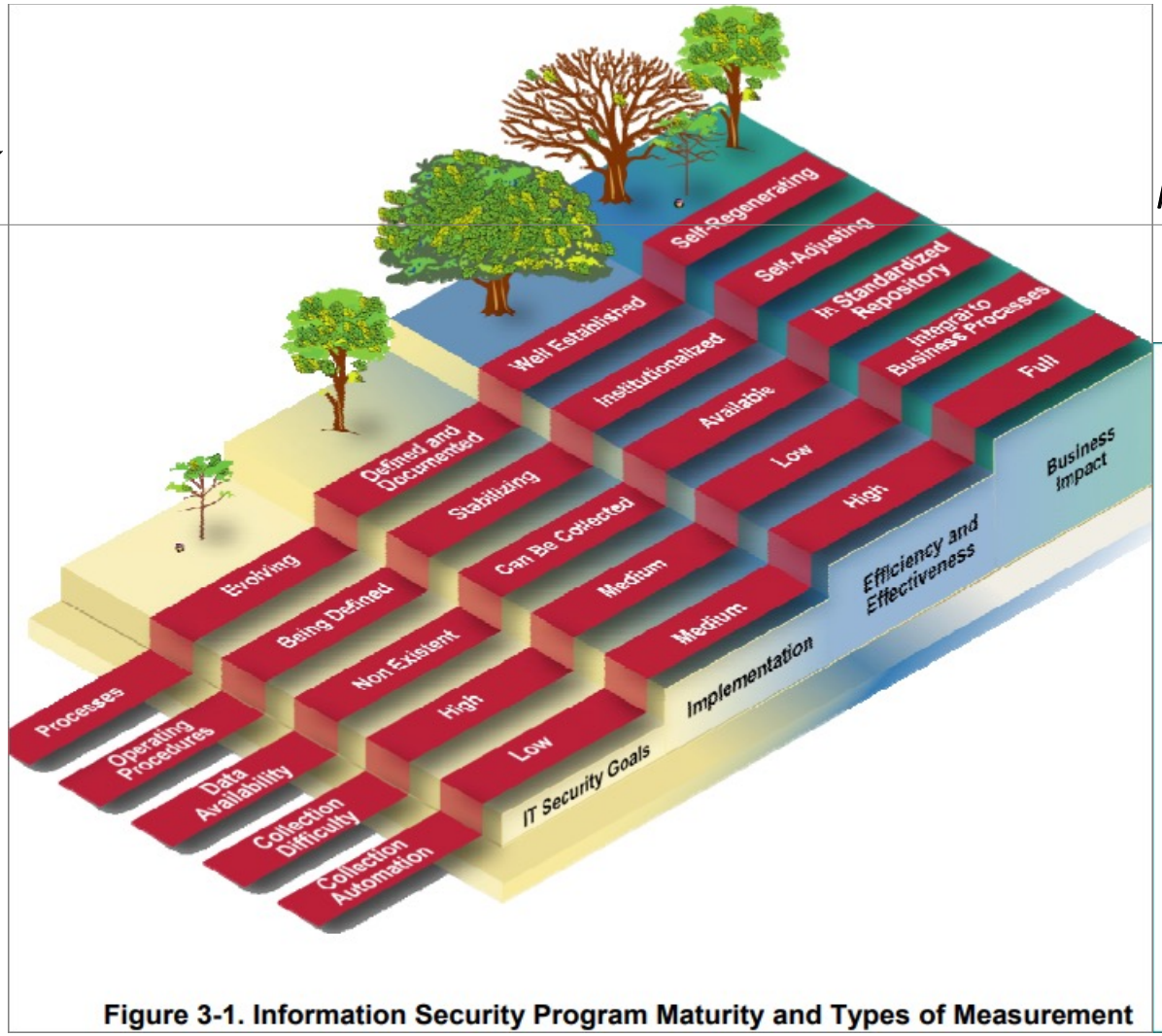
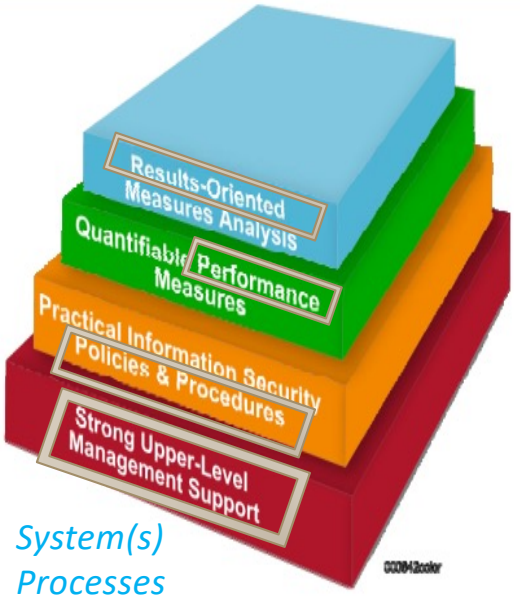


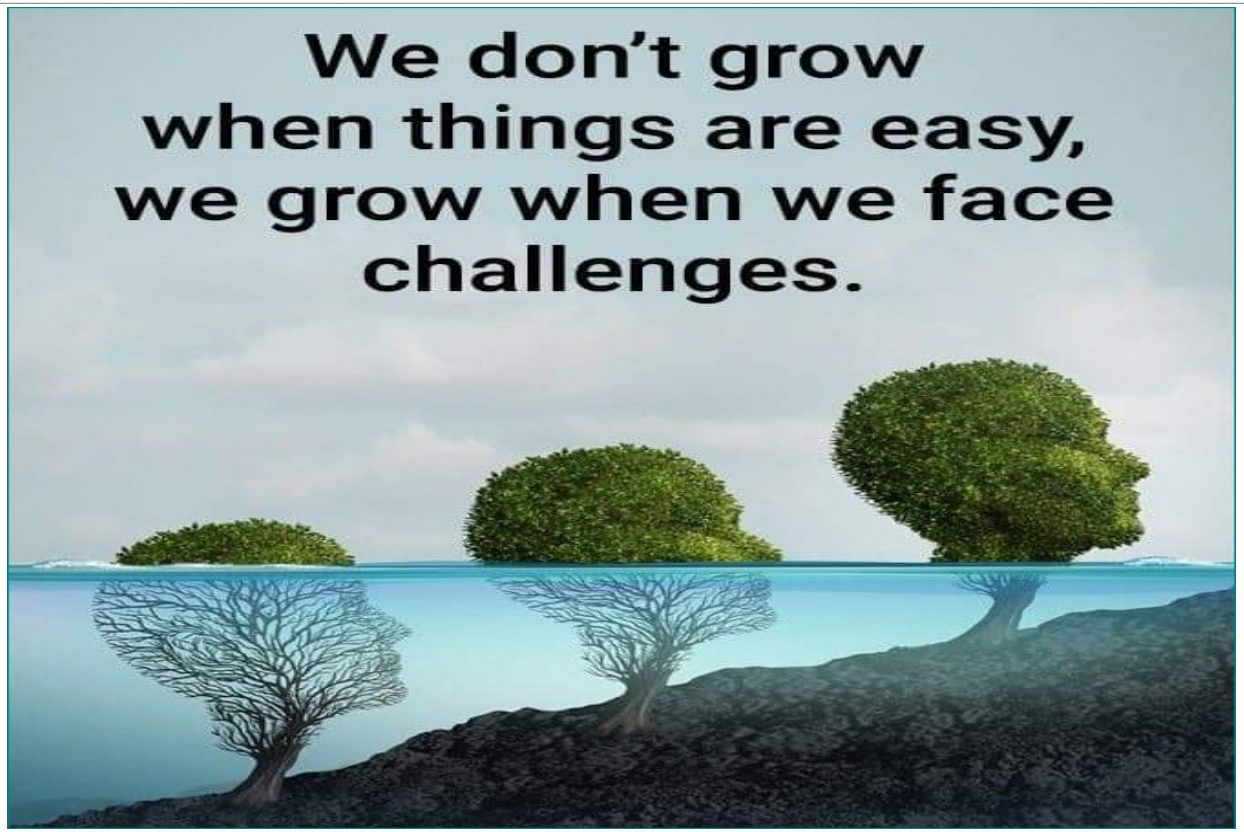
Figure 3-1. Information Security Program Maturity and Types of Measurement



- *System(s)*
- *Processes*
- *SOPs*

Figure 1-1. Information Security Measurement Program Structure

When do we grow?



Parkinson's Law?

The 4-W's:

Why - doing this objective/ project?

- Framework Requirements?

What - will be done & what resources are needed?

- Implementation impacts and the equipment required to perform

Who - is responsible for implementation?

- Identify the personnel's duty in day to day operations

When - is the estimated date of completion?

- SOPs documented, is the objective actually implemented, if not, by when?

Parkinson's Law

If you allow the task to take any amount of your time, then the work will expand proportionally! Parkinson's law says: "Work expands so as to fill the time available for its completion". So! **The more time you allow for your task, the longer it will take to complete it**.

What does RACI stand for?

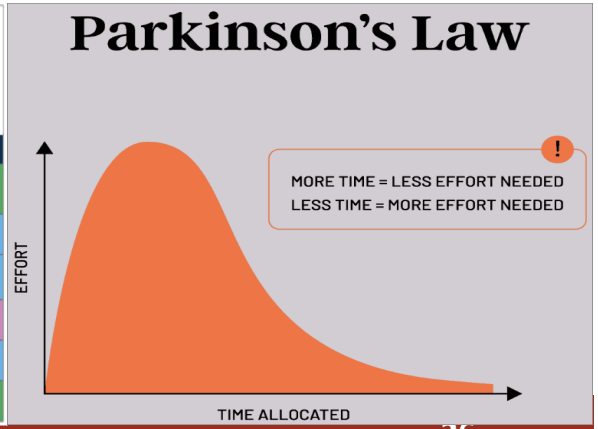
RACI is an acronym for responsible, accountable, consulted, and informed. Each represents the roles and levels of involvement of a stakeholder against the corresponding task/milestone. Let's dive into the definition of each term.

Responsible	Who is *responsible* for doing the actual work for the project task.
Accountable	Who is *accountable* for the success of the task and is the decision-maker. Typically the project manager.*
Consulted	Who needs to be *consulted* for details and additional info on requirements. Typically the person (or team) to be consulted will be the subject matter expert.
Informed	Who needs to be kept *informed* of major updates. Typically senior leadership.

RACI matrix example

R	Responsible
A	Accountable
C	Consulted
I	Informed

Project Activity / Deliverable	Project Manager	Consultant	Architect	Contractor	Client
Define functional and aesthetic needs	I	I	C	I	R
Assess risk	A	R	I	C	I
Define performance requirements	A	R	I	I	I
Create design	A	C	R	I	C
Execute construction	A	C	C	R	I
Approve construction work	I	I	C	C	R



IHS Volatile/ Critical/ Core Controls	Annually Assessed (20 controls)
Account Management	AC-2
Wireless Access	AC-18
Content Of Audit Records	AU-3
Audit Review, Analysis, And Reporting	AU-6
Security Impact Analysis	CM-4
Configuration Settings	CM-6
Least Functionality	CM-7
Information System Component Inventory	CM-8
Configuration Management Plan	CM-9
Contingency Plan	CP-2
Contingency Plan Testing	CP-4
Incident Response Plan	IR-8
Security Planning Policy And Procedures	PL-1
System Security Plan	PL-2
Risk Assessment	RA-3
Vulnerability Scanning	RA-5
System Development Life Cycle	SA-3
Security Engineering Principles	SA-8
Flaw Remediation	SI-2
Malicious Code Protection	SI-3

- ***DIS-CISO Approved as of 24 May 2023***

Small Steps?

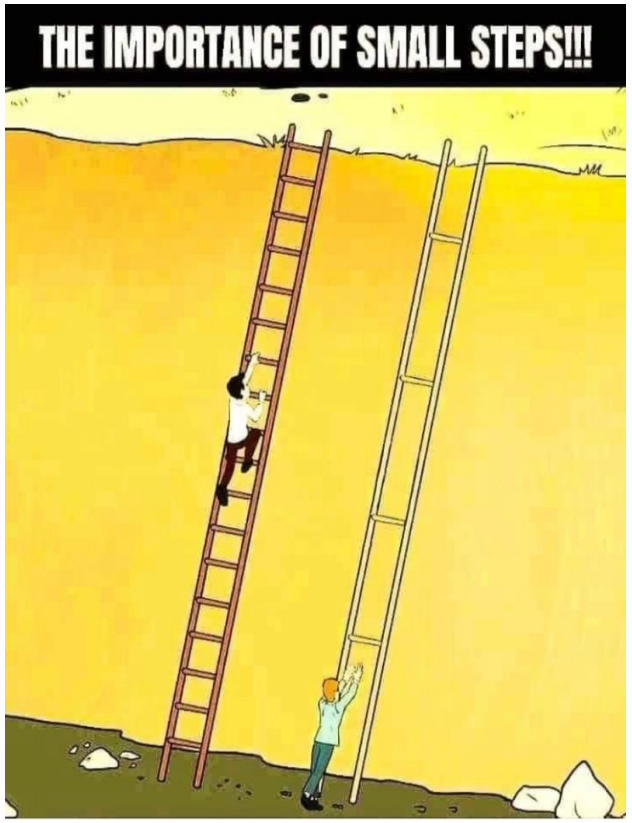
Security is often a combination of multiple small steps and ongoing efforts to protect systems, data, and people.

By breaking down security measures into manageable tasks, we can build a robust security posture and reduce the risk of large-scale breaches or compromises.

Rather than attempting to implement security solutions all at once, it's usually more effective to take small, incremental steps to improve security. This approach allows for careful testing, evaluation, and adjustment along the way, reducing the risk of overlooking critical vulnerabilities or causing significant disruptions.

Here are few examples to illustrate this concept :

- **Regular Updates and Patching**: Keeping software, applications, and systems up to date with the **latest security patches** is crucial. By consistently applying small updates, you can address known vulnerabilities and protect against emerging threats. Neglecting these small steps can expose systems to significant security risks.
- **Employee Training**: Security awareness and **training programs** should focus on small, actionable steps that employees can take to enhance security. This includes practices such as using strong passwords, recognizing phishing attempts, being cautious with email attachments, and reporting suspicious activities. Breaking down security practices into manageable steps increases the likelihood of adoption and compliance.
- **Monitoring and Response**: Effective security often involves constant monitoring and prompt response to security events. By breaking down the detection and response process into smaller steps, security teams can identify and address potential threats in a **timely manner**, preventing or minimizing damage.
- **Network Segmentation**: Dividing a **network into smaller, isolated segments** can enhance security by limiting the impact of a potential breach. If an attacker gains access to one segment, their lateral movement within the network can be restricted, reducing the potential damage they can cause.
- **Secure Development Practices**: In the realm of software development, following secure coding practices and conducting **regular code reviews** can help identify and remedy potential security vulnerabilities early on. By focusing on small, manageable portions of code, developers can identify and fix security issues more effectively.



NIST 800-53, Rev 5 - Control SA-2?

SA-2: Allocation of Resources

Control Family: System and Services Acquisition

CSF v1.1 References: ID.AM-4

PF v1.0 References: GV.PO-P2

Baselines:	
Low	SA-2
Moderate	SA-2
High	SA-2
Privacy	SA-2

Previous Version: NIST Special Publication 800-53 Revision 4: SA-2: Allocation Of Resources

Control Statement

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

Supplemental Guidance

Resource allocation for information security and privacy includes funding for system and services acquisition, sustainment, and supply chain-related risks throughout the system development life cycle.

Related Controls

NIST Special Publication 800-53 Revision 5

- PL-7: Concept of Operations
- PM-3: Information Security and Privacy Resources
- PM-11: Mission and Business Process Definition
- SA-9: External System Services
- SR-3: Supply Chain Controls and Processes
- SR-5: Acquisition Strategies, Tools, and Methods

SA-2: Allocation of Resources

Control Statement:

a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.

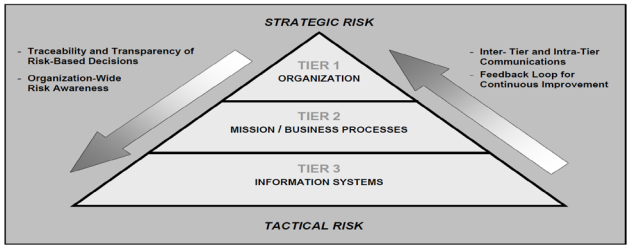
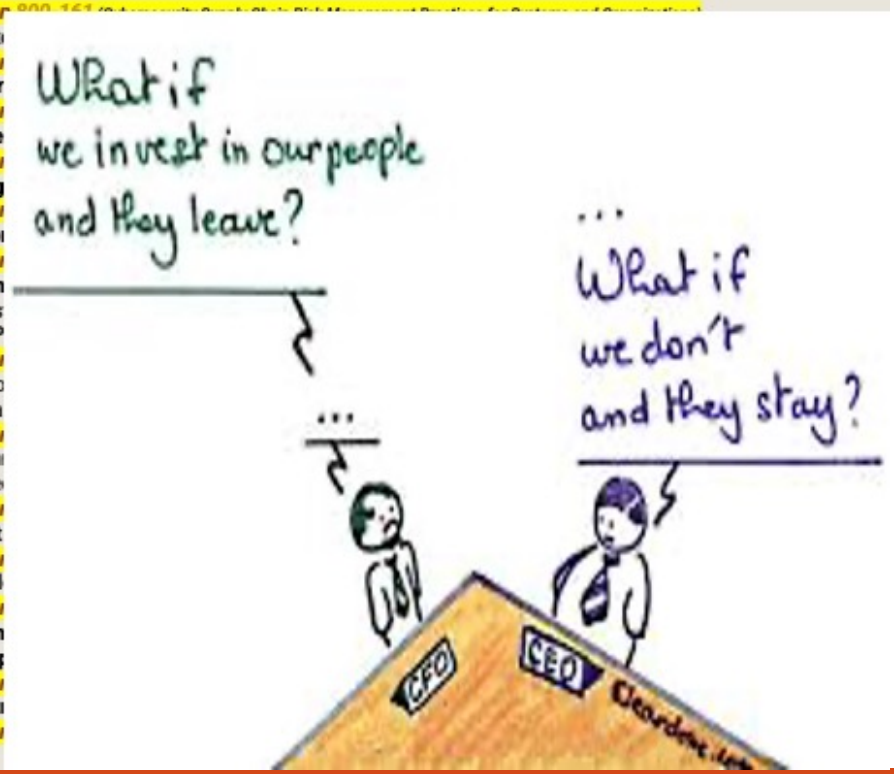


FIGURE 2: MULTITIERED ORGANIZATION-WIDE RISK MANAGEMENT

Training Aids/ NIST Reference(s)

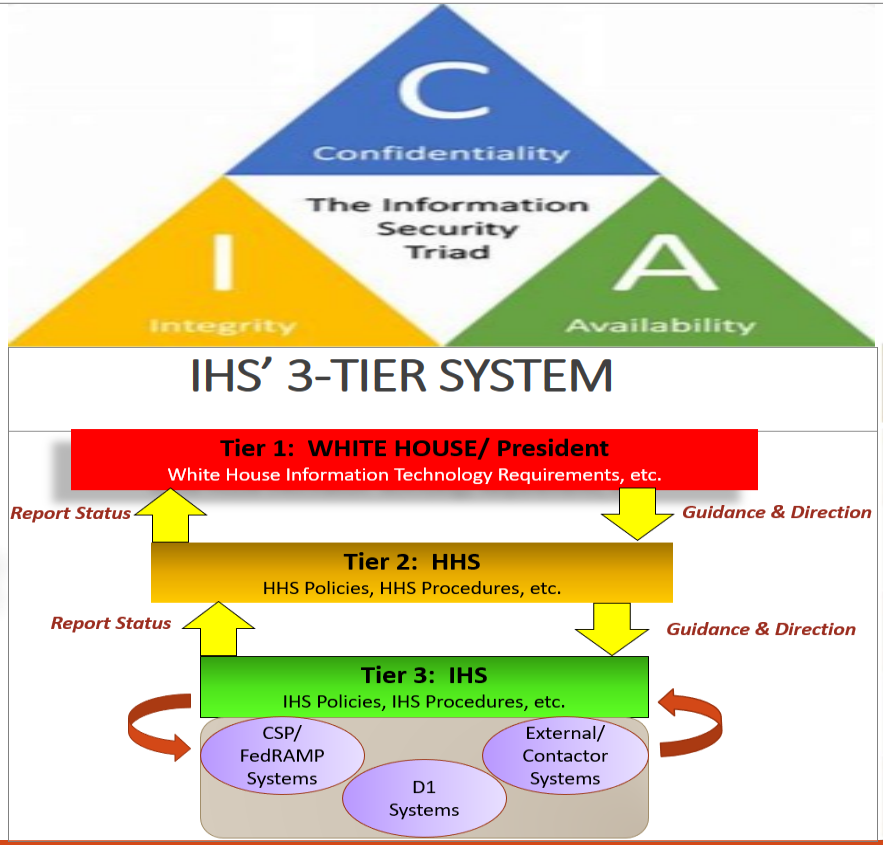
- Supply Chain Risk
  - NIST Special Publicatior
- Strategies to identify and mitigat
  - NIST Special Publicatio
- Development and implementatior
  - NIST Special Publicatio
- Cyber security policies and proce
  - NIST Special Publicatio
- Status and risks, including taking
  - NIST Special Publicatio
- Annual information security repo
  - NIST Special Publicatio
- Development and execution of an security incidents. Reviews inves avoiding similar vulnerabilities. P
  - NIST Special Publicatio
- Monitoring of Information Techno procedures, standards, systems a
  - NIST Special Publicatio
- Monitors timely Information Techi findings. Coordinate policy, proce
  - NIST Special Publicatio
- Identity and access management
  - NIST Special Publicatio
- DevOps ensure security for the cl
  - NIST Special Publicatio
- Development and execution of an Conducts an annual Business Imp
  - NIST Special Publicatio
- Perform annual tabletop crisis st
  - NIST Special Publicatio



IHS' Mission/ Vision/ Goals!

- **Our Mission:** to raise the physical, mental, social, and spiritual health of American Indians and Alaska Natives to the **highest level**
- **Our Vision:** healthy communities and quality health care ***systems*** through strong partnerships and culturally responsive practices
- **Strategic goals:**
  - to ensure that comprehensive, culturally appropriate personal and public health ***services*** are ***available*** and ***accessible*** to American Indian and Alaska Native people;
  - to promote excellence and quality through innovation of the Indian health ***system*** into an **optimally performing** organization; and
  - to strengthen IHS **program management** and **operations**.

Q&A – Discussion/ R&C Contact Info



The End

Presented by	**Sam Tharakan Mathew**
Title	R&C Federal Team Lead/ Manager
Phone	(301) 526-8489
Direct Email	Sam.Mathew@ihs.gov
Team Email	IHSDISRiskAndCompliance@ihs.gov